DATA SHARING CODE OF PRACTICE

Response to consultation from Direct Select (192) Limited t/a ukchanges

ukchanges is a data specialist with over 25 years experience in the marketing data sector. It would come within the category of sharing data as a commercial data broker (as referenced within the draft code of practice). This response therefore is specifically from that commercial perspective.

Our main observation is that we would like to see further detail on the Transparency Requirement, both in terms of the practical obligations of a data controller and also how we can enable data subjects to exercise their rights.

Background legislation

We believe it would be useful for the code to expand on the relevant legislation as follows.

Data Protection Act 2018 Part 3 s.44

We would like to see much greater guidance on how the duties of a controller under this section can be satisfied. The language in s.44 is vague in places - eg it refers to "specific cases" in paragraph (2) without expanding on what they may be.

GDPR Article 14

This concerns the duty of a data controller who has not collected data directly from the data subject. Here, the duty to inform data subjects is subject to the exception where this would be impossible or disproportionate or where it is likely to seriously impair the objectives of the processing.

We feel further guidance on what qualifies as an exception under Article 14 would be beneficial, particularly in the light of the surprising Polish decision in the Bisnode case (albeit a first instance decision subject to appeal).

The draft code

We would make the following points in relation to the draft code:

1. The part of the draft code we see as most relevant to commercial organisations and data brokers is the section starting on page 73, titled "Sharing personal data in databases and lists".

   In particular, we feel the sub-section headed, "What else do we need to do?" would benefit from a much more detailed discussion and guidance on practical obligations, particularly as an interpretation of obligations under the above legislation.

2. It is our view that the exception in GDPR Article 14 paragraph 5(b) would apply in the vast majority of cases where commercial organisations share data but we would appreciate confirmation of this within the Code. Our rationale for this assessment includes the following:

   a. One of the main reasons for the acquisition of databases from third parties and the reason there is a market in this is that is not practical nor commercially viable for

every organisation in the industry to be involved in every step of the data supply chain. Contact with the data subject is the most significant step that some organisations are better placed to carry out than others.

b. The personal data collected does not always include contact details.

c. Data subjects would likely be inundated with approaches from organisations. The majority are unlikely to welcome such approaches, particularly in an era where the reduction in spam is considered positively. Also, vulnerable people or even the average layperson is unlikely to understand the workings of the data industry and may find such information - that they have not expressly sought - confusing or even alarming.

d. A specific example is the Open Register. This is used by a large number of organisations for validating that people live at a stated address. It is also the basis for several marketing products that identify movers or "goneaway" individuals.

   There are in the region of 20 million individuals on the Open Register and thousands of companies that use it. If this sub-section of the draft code were complied with to the letter (if that were possible), that would create a lot of notifications!

e. The requirement to notify is at odds with the ability to rely on legitimate interest. It may even be perceived as a request for consent. For example, it is generally acceptable to rely upon legitimate interest for processing data for postal direct marketing provided the use cases are in line with data subject expectation. If it has already been established that the proposed use is in line with a data subject's expectation, why would it be necessary to notify them?

3. Subject to the above points on a requirement for notification, there is also uncertainty around the timescales for notification set out in Article 14. As personal data can be shared with various organisations and aggregated for the purpose of different database products, at what point would each controller within the supply chain be expected to notify each data subject?

   Also, databases are regularly updated (eg monthly). At what point would it be necessary to notify each data subject that there has been a modification to data held?

4. Is it disproportionate to the rights and freedoms of individuals to have this degree of transparency? Could regular, detailed notifications actually be seen as an intrusion in much the same way as unsolicited emails?

5. Notwithstanding the above, we do appreciate and support that data subjects have a right to transparency and should be able to access information about who is controlling and processing their data, should they wish to do so. However, we are not convinced that that outcome is achieved by imposing the information on a data subject, potentially at frequent intervals.

6. We therefore propose that a solution is sought that enables data subjects to access this information relatively easily but which also addresses the ability of controllers to make it available. For example, we feel there might be scope for creating a data trust that captures sufficient information from controllers to act as a central resource for data subjects to

search in order to find out who holds their information. Something that cuts out duplication, streamlines and simplifies the process for all concerned.

In summary

We would like to see further guidance for commercial organisations on data transparency, guidance that acknowledges the challenges faced within the commercial marketing data sector.

We also feel that a workable solution that addresses the needs of both controllers and data subjects could and should be investigated.

6th September 2019